

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-261549

(43)Date of publication of application : 24.09.1999

(51)Int.Cl.

H04L 9/32
G06F 13/00
H04L 12/54
H04L 12/58

(21)Application number : 10-059485

(71)Applicant : SHARP CORP

(22)Date of filing : 11.03.1998

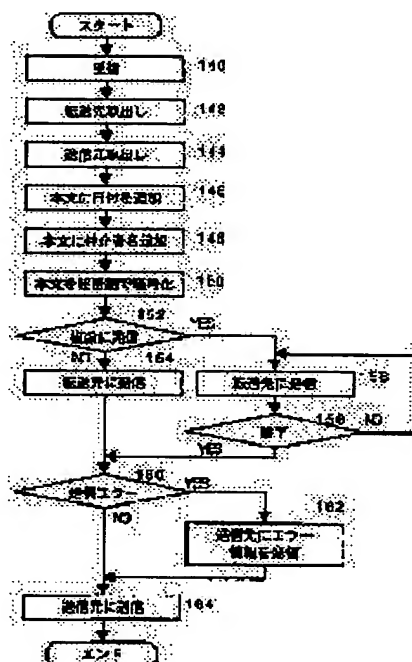
(72)Inventor : YOSHIDA HIROICHI

(54) CONTENT-CERTIFIED ELECTRONIC MAIL DEVICE, METHOD AND STORAGE MEDIUM FOR
CONTENT-CERTIFIED ELECTRONIC MAIL PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a service that corresponds to content-certified mail in an electronic mail system.

SOLUTION: This content-certified electronic mail method includes an electronic mail receiving step (140) that receives an electronic mail and a content-certified transmitting step (142 to 158) which guarantees the identity of the originator of a received electronic mail, a receiving time and content and transmits the received electronic mail to the transfer destination of the received electronic mail. The content-certified transmitting step enciphers a received mail with the secret key of an operator of the electronic mail device (150) and can include a step that allows the operator of the electronic mail device to transmit the mail as an originator to the transfer destination included in the received mail. Preferably, it further includes a return step (164) in which a transmitter also returns an electronic mail that has the same content as the electronic mail sent to the transfer destination to the originator. Both a storage medium that stores a program to accomplish the same purpose and a device are open to the public.



LEGAL STATUS

[Date of request for examination]

12.01.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-261549

(43) 公開日 平成11年(1999) 9月24日

(51) Int.Cl.⁹

識別記号

F I

H 0 4 L 9/32

G 0 6 F 13/00

H 0 4 L 12/54

12/58

3 5 1

H 0 4 L 9/00

G 0 6 F 13/00

H 0 4 L 9/00

11/20

6 7 1

3 5 1 G

6 7 3 B

1 0 1 B

審査請求 未請求 請求項の数11 O L (全 11 頁)

(21) 出願番号

特願平10-59485

(22) 出願日

平成10年(1998) 3月11日

(71) 出願人 000005049

シャープ株式会社

大阪府大阪市阿倍野区長池町22番22号

(72) 発明者 吉田 広市

大阪府大阪市阿倍野区長池町22番22号 シ

ャープ株式会社内

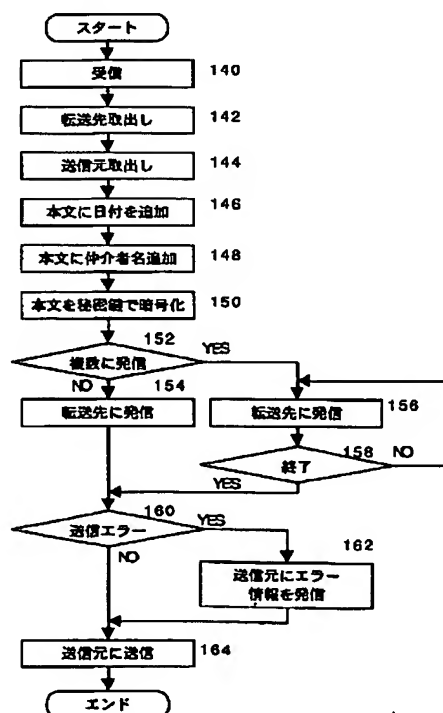
(74) 代理人 弁理士 深見 久郎

(54) 【発明の名称】 内容証明電子メール装置および方法ならびに内容証明電子メールプログラムの記憶媒体

(57) 【要約】

【課題】 内容証明郵便に相当するサービスを電子メールシステムで実現。

【解決手段】 内容証明電子メール方法は、電子メールを受信するための電子メール受信ステップ(140)と、受信した電子メールの発信者、受信時刻および内容の同一性を保証して、受信した電子メールを、受信した電子メールの転送先に送信する内容証明送信ステップ(142~158)とを含む。内容証明送信ステップは、受信したメールを当該内容証明電子メール装置の運用者の秘密鍵で暗号化し(150)、受信したメールに含まれる転送先に当該内容証明電子メール装置の運用者を発信者として送信するステップを含んでもよい。好ましくは、送信装置が転送先に送信する電子メールと同じ内容の電子メールを発信者にも返信するための返信ステップ(164)をさらに含む。同様の目的を達成するためのプログラムを記憶した記憶媒体と、装置とも開示されている。



【特許請求の範囲】

【請求項 1】 電子メールを受信するための電子メール受信手段と、

受信した電子メールの発行者、受信時刻および内容の同一性を保証して、前記受信した電子メールを、前記受信した電子メールの転送先に送信する内容証明送信手段とを含む、内容証明電子メール装置。

【請求項 2】 前記内容証明送信手段は、前記受信したメールを当該内容証明電子メール装置の運用者の秘密鍵で暗号化し、前記受信したメールに含まれる転送先に当該内容証明電子メール装置の運用者を発行者として送信するための送信手段を含む、請求項 1 に記載の内容証明電子メール装置。

【請求項 3】 前記内容証明送信手段は、前記受信した電子メールを当該内容証明電子メール装置の運用者の秘密鍵で暗号化し、前記受信した電子メールに含まれる転送先の全てに当該内容証明電子メール装置の運用者を発行者として送信するための送信手段を含む、請求項 1 に記載の内容証明電子メール装置。

【請求項 4】 前記送信手段が転送先に送信する電子メールと同じ内容の電子メールを当該電子メールの発行者に返信するための返信手段をさらに含む、請求項 2 または請求項 3 に記載の内容証明電子メール装置。

【請求項 5】 さらに、前記内容証明送信手段による転送先への電子メールの送信が失敗したことに応答して、前記受信したメールの発行者に対して電子メールの送信失敗に関する情報を送信するためのエラー情報送信手段を含む、請求項 1 に記載の内容証明電子メール装置。

【請求項 6】 電子メールを受信する電子メール受信ステップと、

受信した電子メールの発行者、受信時刻および内容の同一性を保証して、前記受信した電子メールを、前記受信した電子メールの転送先に送信する内容証明送信ステップとを含む、内容証明電子メール方法。

【請求項 7】 前記電子メール受信ステップは、前記受信したメールを当該内容証明電子メール方法の運用者の秘密鍵で暗号化し、前記受信したメールに含まれる転送先に当該内容証明電子メール方法の運用者を発行者として送信するための送信ステップを含む、請求項 6 に記載の内容証明電子メール方法。

【請求項 8】 前記内容証明送信ステップは、前記受信した電子メールを当該内容証明電子メール装置の運用者の秘密鍵で暗号化し、前記受信した電子メールに含まれる転送先の全てに当該内容証明電子メール装置の運用者を発行者として送信する送信ステップを含む、請求項 6 に記載の内容証明電子メール方法。

【請求項 9】 前記送信ステップが転送先に送信する電子メールと同じ内容の電子メールを当該電子メールの発行者に返信する返信ステップをさらに含む、請求項 7 または請求項 8 に記載の内容証明電子メール方法。

【請求項 10】 さらに、前記内容証明送信ステップによる転送先への電子メールの送信が失敗したことに応答して、前記受信したメールの発行者に対して電子メールの送信失敗に関する情報を送信するためのエラー情報送信ステップを含む、請求項 6 に記載の内容証明電子メール方法。

【請求項 11】 請求項 6 から請求項 10 のいずれかに記載の内容証明電子メール方法を実現するプログラムを機械可読な形式で記録した、内容証明電子メールプログラムの記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は電子メールシステムに関し、特に、既存の郵便システムにおける内容証明郵便に類似した機能を提供することができる電子メールシステムに関する。

【0002】

【従来の技術】ネットワークの普及にともなって、既存の郵便制度と別の電子メールシステムが広く使用されるようになってきている。特に、インターネットの使用が広まることで、異なる組織に属する人でも、互いの組織がインターネットへの接続を行なっていさえすれば、電子メールの授受が可能となってきたこと、および既存の郵便を利用するのと比較して電子メールははるかに手軽に利用できること、により、その利用は増加しつつある。

【0003】一方で、インターネットでは、電子メールに限らず、配信データは複数のコンピュータを介して配送されるため、そのセキュリティに不安があるとされる。そのため、電子メール等を用いたトランザクションをいかに安全に指定された相手に配送するか、について近年多大な労力が払われている。

【0004】それら労力のうちのかかなりの部分が、特に最近のいわゆる「エレクトロニック・コマース」や電子マネーの実用化研究に関連して、情報の盗聴、改ざん、「なりすまし」などと呼ばれる不正行為を防止するための技術に払われている。

【0005】それら技術のうちで、特に脚光を浴びているのがいわゆる暗号化技術である。なかでも、暗号化アルゴリズムが公開されている手法を用いることが、インターネット上で安心して使用できるアルゴリズムの一つの要件であるとされている。暗号化技術の概略の傾向については、「インターネット時代の暗号技術」（三好敏、日経エレクトロニクス、No. 658, 223 頁以下）を参照されたい。

【0006】そうした暗号化技術の一つに、公開鍵を用いたものがある。公開鍵暗号系には、暗号化する際に用いる鍵と、復号する際に用いる鍵との 2 つの鍵が使用される。この二つの鍵は互いに入れ替えても暗号化および復号化が可能である。

【0007】この二つのうちの一つの鍵を公開し（公開

鍵)、他方の鍵を自分など一部の者だけが知っておく(秘密鍵)ようにする。以下、対となる公開鍵と秘密鍵とをまとめて暗号鍵データと呼ぶ。公開鍵は、公開鍵簿と呼ばれるリストに登録され、だれでも知ることができる。こうした暗号鍵データを使用することで、色々なことができる。

【0008】例えば、図9を参照して、ある受信者の暗号鍵データ214が公開鍵220と秘密鍵222を含むものとする。このとき、この受信者とは別の送信者の送信者装置210から当該受信者の装置212に対してインターネットを介して秘密の情報を送信するときは次のような処理を行なう。送信者装置210は、受信者の公開鍵220を用いて情報を暗号化する。インターネット26を介してこの情報を受信した受信者装置212は、この情報を秘密鍵222を用いて復号化する。公開鍵220を用いて暗号化された情報は、秘密鍵222を用いなければ解読できない。したがって、秘密鍵222が人に知られない限り、インターネット26上で情報が盗聴されたとしても直ちにその内容が知られる訳ではない。

【0009】逆に図10を参照して、送信者側の暗号鍵データ230を用いて、送信者の認証を行なうことができる。たとえば、送信者の暗号鍵データ230が秘密鍵240と公開鍵242を含むものとする。秘密鍵240は送信者のみが知っている。公開鍵242は誰でも知ることができる。この場合、送信者装置210で送信情報を秘密鍵240を用いて暗号化し、暗号化された情報をインターネット26を介して受信者装置212に送信する。受信者は、送信者の公開鍵242を用いてこの情報を復号化する。うまく復号化できたら、その情報は秘密鍵240によって暗号化されていたことが分かる。秘密鍵240を知っているのは正しい送信者のみであるから、これによりデータを送信してきた者がその送信者その人であることが分かる。

【0010】

【発明が解決しようとする課題】このように、公開鍵方式を用いた暗号化により、ある程度の信頼性および安全性をもって情報を伝達することができる。しかし、電子メールシステムにおいては、このような暗号化のみによっては解決できない問題がある。

【0011】その一つが、在来の郵便制度で提供されている書留や内容証明郵便(以下まとめて「内容証明郵便」と呼ぶ。)に相当する機能が、従来の電子メールシステムでは提供できなかったという問題である。この問題は、そうしたサービスを提供するためには発信者と受信者との間でこの間のメール送信の仲介を行なう者の存在が必要であるにもかかわらず、従来の電子メールシステムではそうした仲介者となるものがないこと、仮に仲介者となるものがいたとしても、電子メールでは電子データを容易に偽造したり改ざんしたりすることができた

め、書留や内容証明郵便に相当するサービスを提供すること自体が困難と考えられていたこと、による。またこうしたサービスを提供する上で、電子メールの内容をすべて一カ所に記憶しておいたりする手法が考えられないわけではないが、その場合には膨大な容量の外部記憶装置が必要となるという問題がある。さらに、複数の送信先に同一の内容の電子メールを発信する際に、そうした内容証明郵便に相当するサービスが提供できれば便利である。また、そうした内容証明郵便に相当する電子メールの発信の後、その内容が正しいことを確認できると好ましい。また、電子メールの送信にあたって、受信者のメールサーバが故障していたりすると、正常なメールの送信が行なわれない場合がある。この時も、メールの送信が正常に行なわれなかったことを知ることができればさらに好ましい。

【0012】それ故に請求項1または請求項2に記載の発明の目的は、内容証明郵便に相当するサービスを電子メールシステムで実現できる内容証明電子メール装置を提供することである。

20 【0013】請求項3に記載の発明の目的は、複数の宛先に対して同一内容の電子メールを発信する際に内容証明郵便に相当するサービスを電子メールシステムで実現できる内容証明電子メール装置を提供することである。

【0014】請求項4に記載の発明の目的は、内容証明郵便に相当するサービスを電子メールシステムで実現でき、かつ送信された内容を確認できる内容証明電子メール装置を提供することである。

30 【0015】請求項5に記載の発明の目的は、内容証明郵便に相当するサービスを電子メールシステムで実現でき、かつ送信が失敗したことを発信者に通知できる内容証明電子メール装置を提供することである。

【0016】請求項6または請求項7に記載の発明の目的は、内容証明郵便に相当するサービスを電子メールシステムで実現できる内容証明電子メール方法を提供することである。

【0017】請求項8に記載の発明の目的は、複数の宛先に対して同一内容の電子メールを発信する際に内容証明郵便に相当するサービスを電子メールシステムで実現できる内容証明電子メール方法を提供することである。

40 【0018】請求項9に記載の発明の目的は、内容証明郵便に相当するサービスを電子メールシステムで実現でき、かつ送信された内容を確認できる内容証明電子メール方法を提供することである。

【0019】請求項10に記載の発明の目的は、内容証明郵便に相当するサービスを電子メールシステムで実現でき、かつ送信が失敗したことを発信者に通知できる内容証明電子メール方法を提供することである。

50 【0020】請求項11に記載の発明の目的は、請求項6～請求項10に記載の、内容証明郵便に相当するサービスを電子メールシステムで実現できる内容証明電子メ

ール方法を実現する内容証明電子メールプログラムの記憶媒体を提供することである。

【0021】

【課題を解決するための手段】請求項1に記載の発明にかかる内容証明電子メール装置は、電子メールを受信するための電子メール受信手段と、受信した電子メールの発行者、受信時刻および内容の同一性を保証して、受信した電子メールを、受信した電子メールの転送先に送信する内容証明送信手段とを含む。

【0022】受信した電子メールの発行者と、受信時刻と、その内容との同一性を保証して転送先に送信する内容証明送信手段により、発行者とは異なる第三者によって、その電子メールの内容証明が提供される。

【0023】請求項2に記載の発明にかかる内容証明電子メール装置は、請求項1に記載の発明の構成に加えて、内容証明送信手段は、受信したメールを当該内容証明電子メール装置の運用者の秘密鍵で暗号化し、受信したメールに含まれる転送先に当該内容証明電子メール装置の運用者を発行者として送信するための送信手段を含む。

【0024】内容証明電子メール装置の運用者の秘密鍵は、当該運用者にしか知られない。したがってその運用者から発信された電子メールを当該運用者の公開鍵で復号化できれば、その電子メールは確かに当該運用者から送信されたものであることが分かる。したがってその電子メールの内容証明の信ぴょう性を高めることができる。

【0025】請求項3に記載の発明にかかる内容証明電子メール装置は、請求項1に記載の発明の構成に加えて、内容証明送信手段は、受信した電子メールを当該内容証明電子メール装置の運用者の秘密鍵で暗号化し、受信した電子メールに含まれる転送先の全てに当該内容証明電子メール装置の運用者を発行者として送信するための送信手段を含む。

【0026】内容証明電子メール装置が、複数の転送先のすべてに電子メールを送信するので、発行者は、1通の電子メールと、必要な転送先の宛名とを内容証明電子メール装置に対して発信すればよく、簡単に複数の相手に対して内容証明された電子メールを送ることができる。

【0027】請求項4に記載の発明にかかる内容証明電子メール装置は、請求項2または請求項3に記載の発明の構成に加えて、送信手段が転送先に送信する電子メールと同じ内容の電子メールを当該電子メールの発行者に返信するための返信手段をさらに含む。

【0028】転送先に送信されたのと同じ電子メールを発行者に対して送信することで、発行者は内容証明のメールが受信者に転送されたことを知ることができる。しかも返送される電子メールは内容証明電子メール装置の運用者の秘密鍵で暗号化されている。したがって当該電

子メールが確かに内容証明電子メール装置から返送されたものであることが保証され、その電子メールを発行者が保持しておくことで、その内容証明を行なうことができる。またこれにより内容証明電子メール装置自体は、内容証明したメールのコピーを保持しておく必要がなくなり、大量の電子メールを処理したとしても、外部記憶装置などの資源が不足するおそれは少ない。

【0029】請求項5に記載の発明にかかる内容証明電子メール装置は、請求項1に記載の発明の構成に加えてさらに、内容証明送信手段による転送先への電子メールの送信が失敗したことに応答して、受信したメールの発行者に対して電子メールの送信失敗に関する情報を送信するためのエラー情報送信手段を含む。

【0030】内容証明のメールの送信に失敗したことが発行者に対して通知されるので、発行者は適切な対応をすることが可能になる。

【0031】請求項6に記載の発明にかかる内容証明電子メール方法は、電子メールを受信する電子メール受信ステップと、受信した電子メールの発行者、受信時刻および内容の同一性を保証して、受信した電子メールを、受信した電子メールの転送先に送信する内容証明送信ステップとを含む。

【0032】受信した電子メールの発行者と、受信時刻と、その内容との同一性を保証して転送先に送信する内容証明送信ステップにより、発行者とは異なる第三者によって、その電子メールの内容証明が提供される。

【0033】請求項7に記載の発明にかかる内容証明電子メール方法は、請求項6に記載の発明の構成に加えて、電子メール受信ステップは、受信したメールを当該内容証明電子メール方法の運用者の秘密鍵で暗号化し、受信したメールに含まれる転送先に当該内容証明電子メール方法の運用者を発行者として送信するための送信ステップを含む。

【0034】内容証明電子メール方法の運用者の秘密鍵は、当該運用者にしか知られない。したがってその運用者から発信された電子メールを当該運用者の公開鍵で復号化できれば、その電子メールは確かに当該運用者から送信されたものであることが分かる。したがってその電子メールの内容証明の信ぴょう性を高めることができる。

【0035】請求項8に記載の発明にかかる内容証明電子メール方法は、請求項6に記載の発明の構成に加えて、内容証明送信ステップは、受信した電子メールを当該内容証明電子メール装置の運用者の秘密鍵で暗号化し、受信した電子メールに含まれる転送先の全てに当該内容証明電子メール装置の運用者を発行者として送信する送信ステップを含む。

【0036】内容証明電子メール方法により、複数の転送先のすべてに電子メールが送信されるので、発行者は、1通の電子メールと、必要な転送先の宛名とを内容

証明電子メール方法の運用者に対して発信すればよく、簡単に複数の相手に対して内容証明された電子メールを送ることができる。

【0037】請求項9に記載の発明にかかる内容証明電子メール方法は、請求項7または請求項8に記載の発明の構成に加えて、送信ステップが転送先に送信する電子メールと同じ内容の電子メールを当該電子メールの発信者に返信する返信ステップをさらに含む。

【0038】転送先に送信されたのと同じ電子メールを発信者に対して送信することで、発信者は内容証明のメールが受信者に転送されたことを知ることができる。しかも返送される電子メールは内容証明電子メール方法の運用者の秘密鍵で暗号化されている。したがって当該電子メールが確かに内容証明電子メール方法の運用者から返送されたものであることが保証され、その電子メールを発信者が保持しておくことで、その内容証明を行なうことができる。またこれにより内容証明電子メール方法を運用する装置自体は、内容証明したメールのコピーを保持しておく必要がなくなり、大量の電子メールを処理したとしても、外部記憶装置などの資源が不足するおそれは少ない。

【0039】請求項10に記載の発明にかかる内容証明電子メール方法は、請求項6に記載の発明の構成に加えてさらに、内容証明送信ステップによる転送先への電子メールの送信が失敗したことに応答して、受信したメールの発信者に対して電子メールの送信失敗に関する情報を送信するためのエラー情報送信ステップを含む。

【0040】内容証明のメールの送信に失敗したことが発信者に対して通知されるので、発信者は適切な対応をすることが可能になる。

【0041】請求項11に記載の発明にかかる内容証明電子メールプログラムの記憶媒体は、請求項6から請求項10のいずれかに記載の内容証明電子メール方法を実現するプログラムを機械可読な形式で記録したものである。

【0042】この記憶媒体に記憶されたプログラムをコンピュータに実行させることにより、請求項6から請求項10に記載した発明と同様の効果を得ることができる。

【0043】

【発明の実施の形態】図1を参照して、本願発明の一実施の形態の電子メールシステムは、互いにインターネット26に接続された送信者装置20および受信者装置24に加えて、送信者装置20から受信者装置24への内容証明電子メールを仲介するための仲介者装置22を含む。本実施の形態では、送信者が、秘密鍵40および公開鍵42を含む暗号鍵データ30を有し、仲介者が、秘密鍵44および公開鍵46を含む暗号鍵データ32を有しているものとする。

【0044】なお、送信者がこのように自分の暗号鍵デ

ータ30を持っていることは仲介者装置22による内容証明の処理にとっては関係なく、なくとも構わない。

【0045】発信者装置20は、全体を管理するための処理を行なうプログラムを実行するCPU50と、文字を入力するための入力装置52と、入力された情報を表示するための表示装置54と、入力された文字を編集するための編集装置56と、編集されたデータを送受信するための通信装置60と、表示プログラム、編集プログラム、暗号化および復号化プログラムならびに各処理に使用されるデータが格納されるRAM62と、表示プログラム、編集プログラム、暗号化および復号化プログラムなどを記録した記憶媒体64等からプログラム、データなどを読み取り、RAM62に格納するための外部記憶装置58とを含む。

【0046】受信者装置24も、送信者装置20と同じ構成を有するので、ここではその詳細はくり返さない。

【0047】図3を参照して、仲介者装置22は、全体を管理するための処理を行なうプログラムを実行するCPU70と、電子メールを受信するための受信装置72と、電子メールを送信するための送信装置80と、電子メールを暗号化するための暗号装置74と、送信された電子メールを一時的に保持するためのデータバッファ82と、電子メールがこの仲介者装置22を通過した時間をスタンプするための時計76と、発信者情報と受信者情報とを保存するためのバッファ84と、暗号装置74を実現するためのプログラム88を記憶するためのRAM86と、当該暗号化プログラムを機械可読な形式で記憶した記憶媒体90から暗号化プログラムを読み出し、RAM86に格納するための外部記憶装置78とを含む。

【0048】データの流れは以下ようになる。図4を参照して、送信者装置20では、送信内容100を自己の秘密鍵40を用いて暗号化する。暗号化した送信内容102を電子メールで仲介者装置22に宛てて送る。このとき、真の送信先（受信者）を転送先として電子メール中で指定しておく。

【0049】仲介者装置22は、受信したメールのデータにそのメールの受信日付および仲介者の名称を付加し、さらに自己の秘密鍵44を用いて暗号化する。仲介者装置22は、このようにさらに暗号化した送信内容104を、指定された転送先である受信者装置24に宛てて電子メールで送信する。受信者装置24は、仲介者装置22から電子メールを受け取ると、仲介者装置22の公開鍵46を用いて復号化する。公開鍵46で電子メールを復号化できれば、この電子メールが仲介者装置22から送られてきたものであることが確認できる。この場合、復号化することにより発信者装置20で暗号化された送信内容106が得られるので、必要であればこの送信内容をさらに復号化すれば必要な情報が得られる。

【0050】また、仲介者装置22は、受信者装置24

に宛てて送信した送信内容 1 0 4 と同じ送信内容 1 0 8 を電子メールで送信者装置 2 0 に宛てて送信する。発信者装置 2 0 は、この電子メールを仲介者 2 2 の公開鍵を用いて復号化して、自己が暗号化した送信内容 1 1 0 を得る。この送信内容をさらに復号化して得られた送信内容 1 1 2 が、最初の送信内容 1 0 0 と等しければ、正しい内容の電子メールが受信者装置 2 4 に向けて送信されてことが分かる。また、発信者装置 2 0 が受けた電子メールの送信内容 1 0 8 は、仲介者装置 2 2 から受信者装置 2 4 に向けて送信された送信内容 1 0 4 と同じものである。この送信内容 1 0 8 は、仲介者の秘密鍵によって暗号化されたものである。したがって、この送信内容 1 0 8 を保持しておくことで、発信者装置 2 0 は、仲介者装置 2 2 によって、電子メールの内容証明に相当するサービスを受けられることになる。

【0 0 5 1】図 5 を参照して、発信者装置 2 0 において実行される処理の流れは以下になる。まず、送信すべきメールを作成する (1 2 0)。このメール自体の内容を秘密にしておくべきであれば (1 2 2 の判断で YES) このメールを暗号化する (1 2 4)。その上で、このメールを内容証明で送るべきか否かを判断し (1 2 6)、内容証明を用いないときには宛名を受信者にして (1 2 8) 送信する (1 3 2)。内容証明で送るときには、宛名を仲介者に、転送先を受信者に、それぞれ指定して (1 3 0)、メールを送信する (1 3 2)。これで発信時における発信者側装置の処理は終了である。

【0 0 5 2】図 6 を参照して、仲介者装置 2 2 における処理は以下のとおりである。まず、電子メールを受信する (1 4 0)。この電子メールから転送先の宛名を取り出し (1 4 2)、発信者の宛名を取り出す (1 4 4)。次に送信されてきた電子メール本文に、受け取った日付けを追加し (1 4 6)、さらに仲介者名を追加 (1 4 8) する。次に、この電子メール全体を仲介者自身の秘密鍵 4 4 (図 1 を参照) で暗号化する (1 5 0)。

【0 0 5 3】次に、転送先が複数あるか否かをチェックする (1 5 2)。転送先がひとつだけであればその転送先に発信する (1 5 4)。転送先が複数個あれば、そのすべてに対してこの電子メールを発信する (1 5 6、1 5 8)。

【0 0 5 4】このようにして行なった電子メールの発信処理の結果、送信エラーがあったか否かを判定する (1 6 0)。送信エラーがあれば、発信者に対して転送エラー情報を発信する (1 6 2)。

【0 0 5 5】最後に、ステップ 1 5 4 またはステップ 1 5 6 で転送先に発信したものと同一電子メールを発信者に対しても送信する (1 6 4)。以上で仲介者装置で行なわれる処理は終了である。

【0 0 5 6】受信者装置では、電子メールの受信時に以下のような処理が行なわれる。図 7 を参照して、まず電子メールを受信する (1 7 0)。受信した電子メールの

送信者が仲介者装置 2 2 か否かを判定する (1 7 2)。仲介者からのメールでない場合には処理はステップ 1 7 6 に進む。仲介者からのメールであればこの電子メールが内容証明のメールとして送られて来たことを認識し、電子メールの内容を仲介者の公開鍵 4 6 (図 1 参照) で復号化する (1 7 4)。

【0 0 5 7】次に、ステップ 1 7 6 で、電子メールの内容の発信者と発信時間とを確認する。そして、その内容が暗号化されているかどうかを判定する (1 7 8)。暗号化されていればその内容を復号化する。こうして得られたメールの内容を確認して (1 8 2) 処理を終了する。このようにして、受信者装置では、仲介者装置から送信されてきた電子メールが内容証明のメールであることを知ることができる。

【0 0 5 8】一方、発信者装置 2 0 では、図 6 のステップ 1 6 4 で仲介者装置 2 2 から返信されたメールを受け取り以下のような処理を行なう。図 8 を参照して、発信者装置 2 0 は、電子メールを受け取ると (1 9 0)、その発信者が仲介者であるか否かを判定する (1 9 2)。発信者が仲介者でなければ処理はステップ 1 9 8 に進む。ステップ 1 9 8 以下の処理については後述する。発信者が仲介者であれば、以前に内容証明のメールとして送信したメールが受信者に対して内容証明のメールとして仲介者から発信されたことが分かる。この場合、発信者装置 2 0 は、そのメールを一旦コピーし (1 9 4)、コピーしたものの内容を仲介者の公開鍵 4 6 (図 1 参照) を用いて復号化する (1 9 6)。その後処理はステップ 1 9 8 に進む。

【0 0 5 9】ステップ 1 9 8 では、電子メールの本文が暗号化されているか否かを判定する。本文が暗号化されていればその内容を自己の公開鍵で復号化する (2 0 0)。こうして得られた電子メールの内容につき、その内容が自己が発信した内容と一致するか否かを判定する (2 0 2)。一致していれば処理が正常に行なわれたと言えるから、メールを保存し (2 0 4) 処理を終了する。一致しなければどこかで問題が生じたということであるから (2 0 6)、何らかの対応をとる。

【0 0 6 0】このような仲介者装置 2 2 を用いた電子メールシステムにより、在来の郵便物における郵便局の内容証明郵便と同様に、どのような内容の電子メールを、いつ、誰に送信したかを証明することができる。また上記したように転送先として複数を指定できるようにしておき、仲介者装置でその複数の転送先の各々に対して内容証明に必要な処理を行なうことにより、発信者は 1 通の電子メールと複数の宛名とを用意し発信するだけで、同じ内容の複数の電子メールを、異なる宛先に内容証明のメールとして発信させることができる。

【0 0 6 1】また上記した実施の形態のシステムでは、受信者に対して送信したのと同じ内容の電子メールを仲介者装置から発信者に対して返送している。こうするこ

とで、発信者は自己の電子メールが内容証明のメールとして受信者に対して発信されたことが分かるが、その内容が仲介者の秘密鍵で暗号化されていることから、そのメールが確かに仲介者装置によって発信されたものであることを証明できる。同じ内容の電子メールが受信者に対して発信されたことは仲介者において証明できるから、結局、発信者から受信者に対して送信された電子メールの内容が、仲介者から発信者に対して返送された電子メールの内容と同一であることが証明できることになる。またこの場合、仲介者装置としては、内容証明した電子メールを発信者に対して返送すればよく、内容証明のために自己にそのコピーを保存する必要がない。そのため、仲介者装置にデータを蓄積する必要がなくなり、多数のメールを処理した場合でも外部記憶装置などの資源の不足が生ずるということはない。

【0062】また、仲介者装置から発信する際に何らかの送信エラーがあった場合、仲介者装置から発信者に対して送信エラー情報が送信される。そのため、たとえばメールサーバ等に故障があって電子メールの送付が正常に行なえなかった場合、発信者がそうした異常を知ることができ、適切な処理をとることが可能である。

【0063】本願発明にかかる装置および方法を、一実施の形態のシステムに基づいて説明してきたが、本願発明の技術的範囲が上述した実施の形態のシステムに限定されないことはもちろんであり、上記以外にも様々な修正をして実施することができる。

【図面の簡単な説明】

【図1】図1は、本願発明の一実施の形態にかかる電子メールシステムの全体構成を示す模式図である。

【図2】図2は、本願発明の一実施の形態にかかる電子メールシステムで用いられる送信者装置のブロック図である。

【図3】図3は、本願発明の一実施の形態にかかる電子

メールシステムで用いられる、仲介者装置のブロック図である。

【図4】図4は、本願発明の一実施の形態にかかる電子メールシステムにおける電子メールのデータの流れを示す模式図である。

【図5】図5は、本願発明の一実施の形態にかかる電子メールシステムにおいて用いられる送信者装置の、メールの送信時のプログラム処理のフローチャートである。

【図6】図6は、本願発明の一実施の形態にかかる電子メールシステムにおいて用いられる仲介者装置のプログラム処理のフローチャートである。

【図7】図7は、本願発明の一実施の形態にかかる電子メールシステムにおいて用いられる受信者装置の、メールの受信時のプログラム処理のフローチャートである。

【図8】図8は、本願発明の一実施の形態にかかる電子メールシステムにおいて用いられる送信者装置の、仲介者装置からのメールの受信時のプログラム処理のフローチャートである。

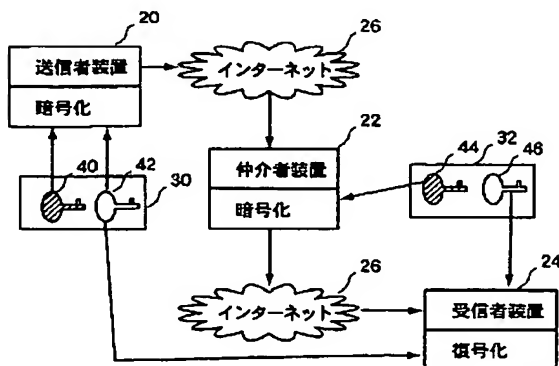
【図9】図9は、従来の電子メールシステムにおける公開鍵システムの使用法を示す模式図である。

【図10】図10は、従来の電子メールシステムにおける公開鍵システムの他の使用法を示す模式図である。

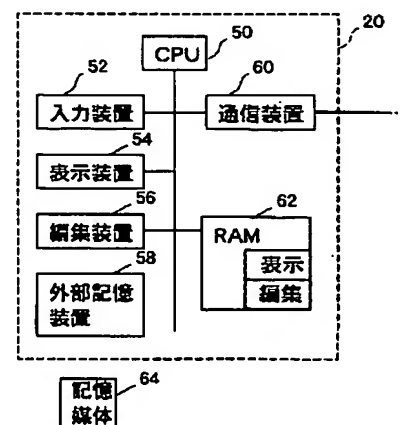
【符号の説明】

- 20 送信者装置
- 22 仲介者装置
- 24 受信者装置
- 26 インターネット
- 50、70 CPU
- 60 通信装置
- 58、78 外部記憶装置
- 62、86 RAM
- 64、90 記憶媒体

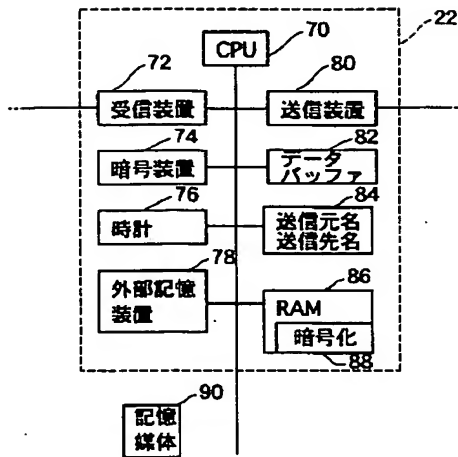
【図1】



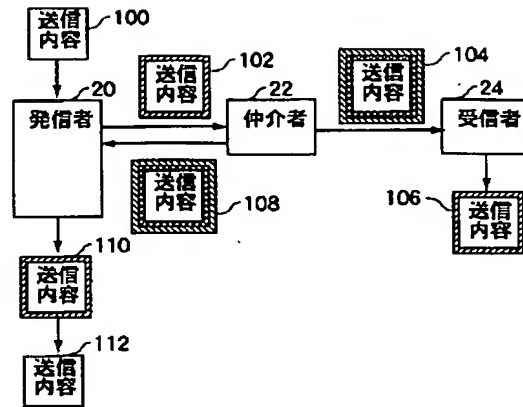
【図2】



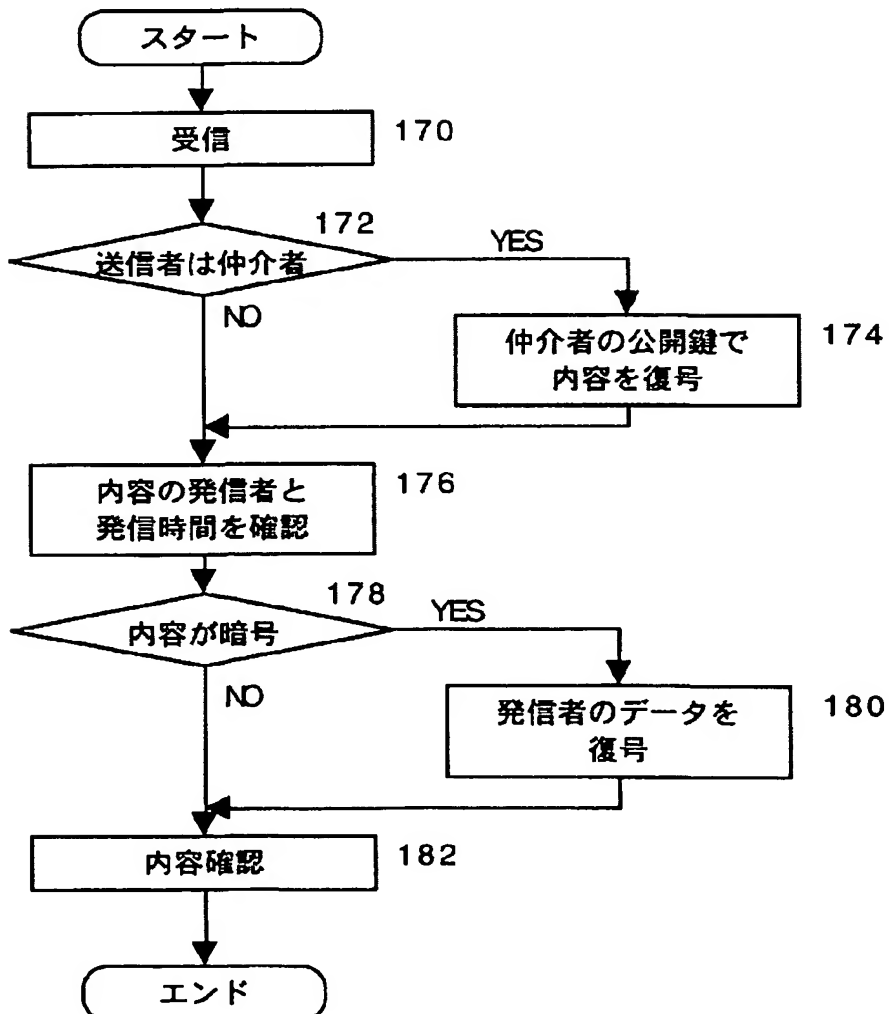
【図3】



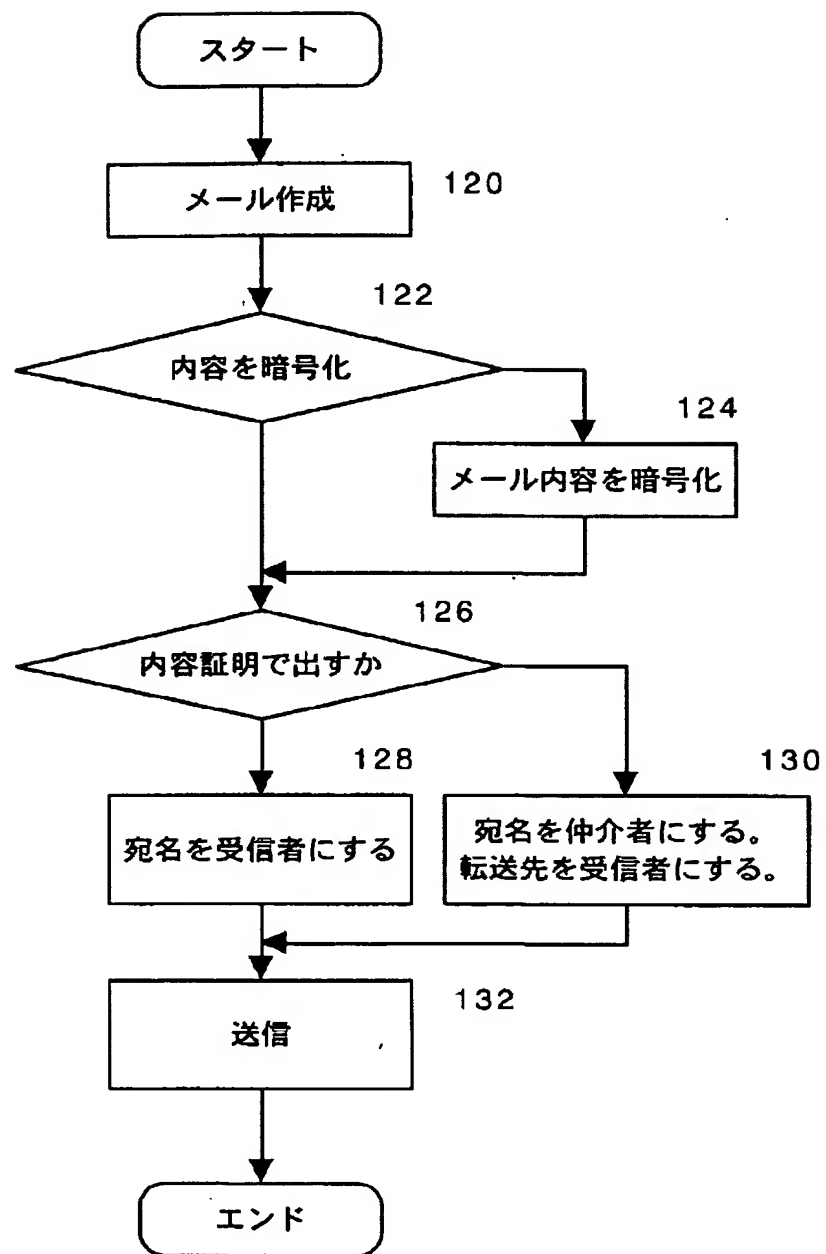
【図4】



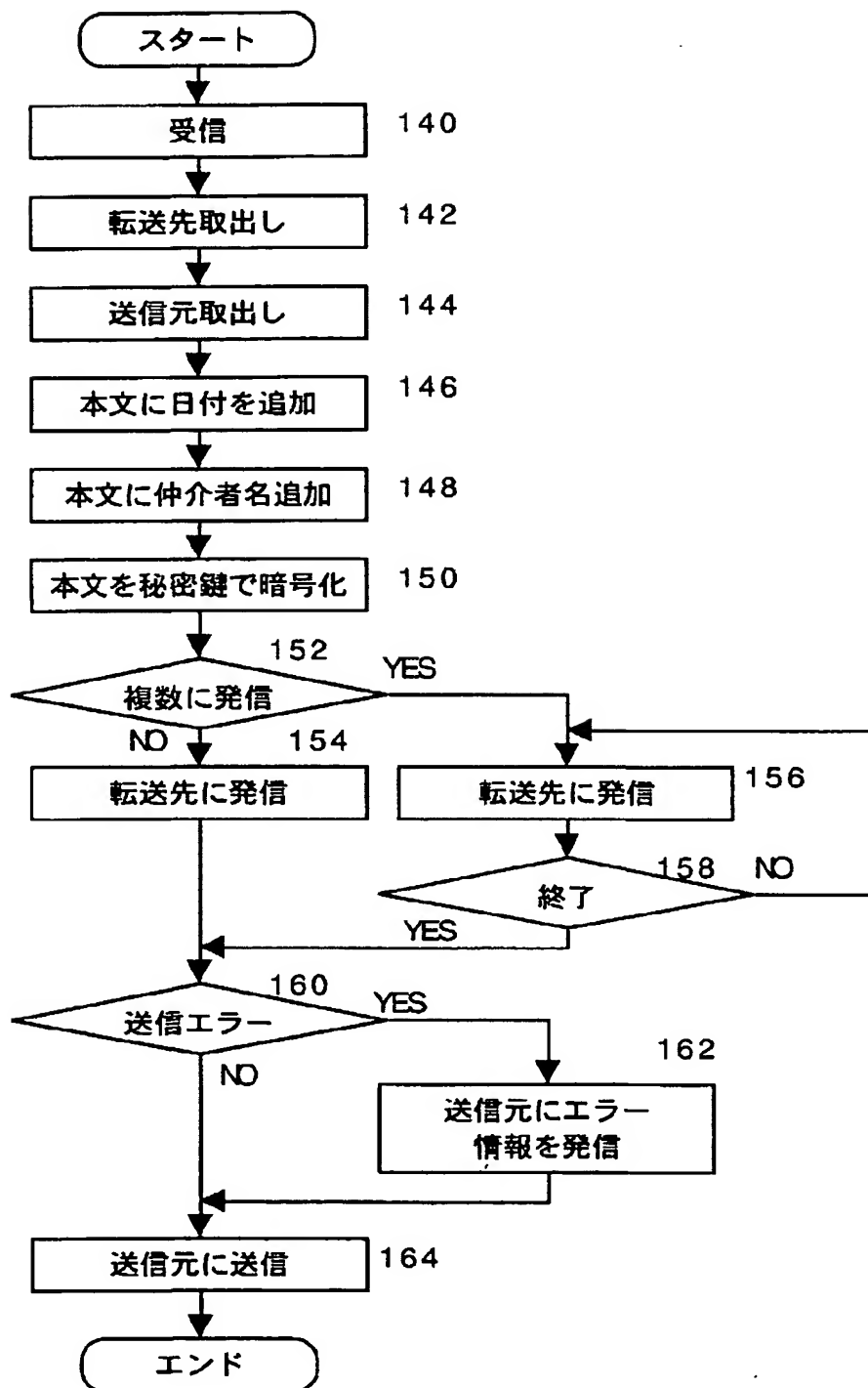
【図7】



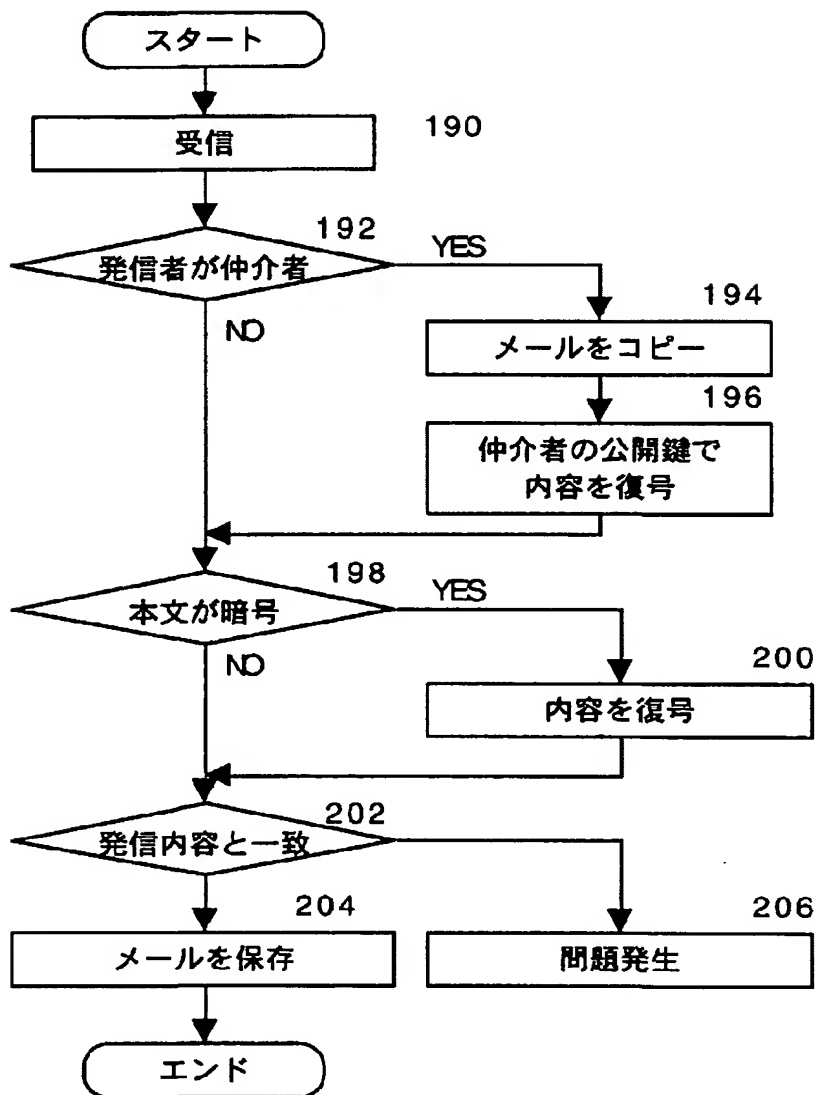
【図 5】



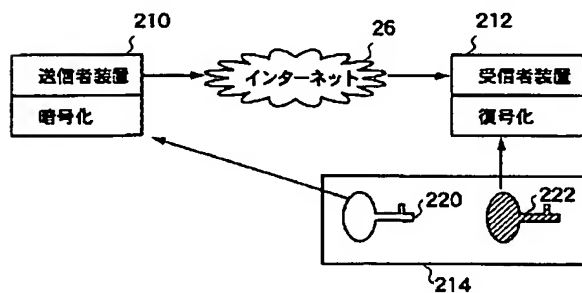
【図 6】



【図 8】



【図 9】



【図 10】

